Confidential

ZSCALAR:PROXY SUSPICIOUS COMMUNICATION

TCS Internal

Confidential

Confidential

Why do we use proxy?

- The job of a Proxy is to provide a gateway between the users and the internet.
- A good quality, well configured proxy assists in keeping users and the internal network protected from the unwanted content published and accessible on the internet.
- Proxy logs contain a lot of valuable data which can be used for detecting suspicious activity.

TCS Internal

Confidential

Confidential

Event Name: Zscalar:Proxy Suspicious Communication

Rule Description

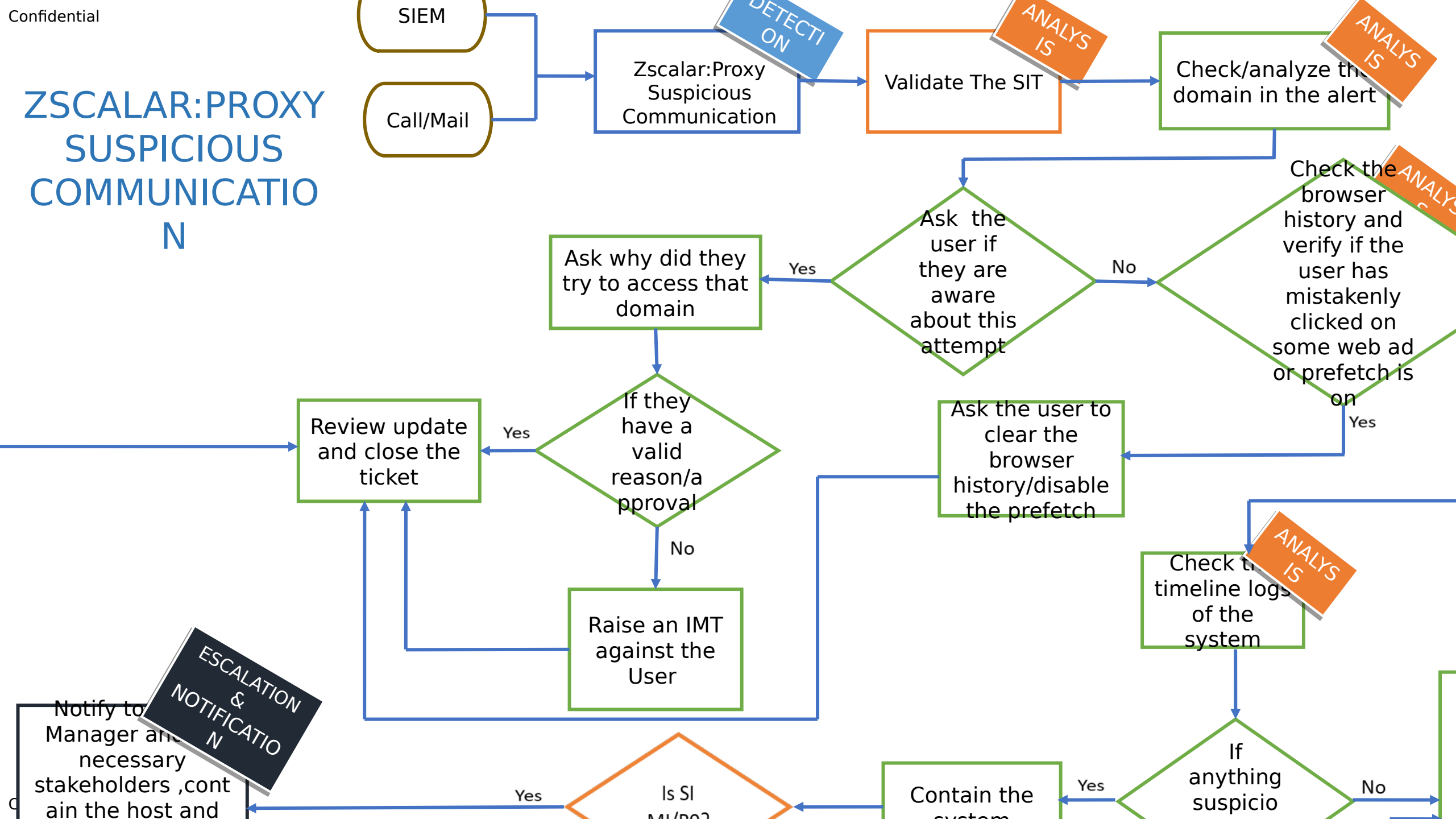
- Apply UC:001:Zscalar:Proxy_Suspicious Communication on events which are detected by the Local system.
- and when the event(s) were detected by one or more of Zscaler Nss.
- and when the event matches ActualAction (custom) is any of Allowed.
- and when any of BC_ParentDomain (custom) are contained in any of RF - Domain - Score - AlphaNumeric (Ignore Case), TCS_CSO_Domains - AlphaNumeric (Ignore Case)
- and NOT when any of BC_ParentDomain (custom) are contained in any of TCS_Legitimate domains - AlphaNumeric (Ignore Case)
- and NOT when any of URL (custom) is the key and any of Username is the value in any of TCS_legitimate url wrt to users - AlphaNumeric

TCS Internal

Confidential

Confidential

ZSCALAR:PROXY SUSPICIOUS COMMUNICATION



Confidential

Questions/Queries to be asked

- Verify with the user whether they are aware about this attempt.
- Ask the purpose for accessing the domain.
- Do they have appropriate approval for accessing the domain.
- Confirm if they tried to download anything from that domain.

TCS Internal

Confidential